UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/645,588	08/25/2000	Seigo Arita	040405/0326	3989

22428 7590 05/06/2004

FOLEY AND LARDNER
SUITE 500
3000 K STREET NW
WASHINGTON, DC 20007

EXAMINER	
DADA, BEEMNET W	
ART UNIT	PAPER NUMBER
2135	5

DATE MAILED: 05/06/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/645,588	**Applicant(s)** ARITA, SEIGO	
	Examiner Beemnet W Dada	**Art Unit** 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 August 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-39* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *3*.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-39 have been examined.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 36-39 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

4. Claim 36 recites the limitation "said Stickelberger element computing procedure" in line 5. There is insufficient antecedent basis for this limitation in the claim.

5. Claim 37 recites the limitation "said Jacobian addition candidate value computing procedure" in lines 5-6. There is insufficient antecedent basis for this limitation in the claim.

6. Claim 38 recites the limitation "said order candidate value computing procedure" in lines 5-6. There is insufficient antecedent basis for this limitation in the claim.

7. Claim 39 recites the limitation "said parameter deciding procedure" in line 5. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1-35 and 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Duursma et al. (hereinafter Duursma) (ref U) in view of Stevens (ref V).

9. As per claims 1,18 and 35 Duursma teaches a secure parameter generating method in an algebraic curve (hyperelliptic curve), comprising the steps of:

a Jacobian addition candidate value computing procedure for computing Jacobian addition candidate value j corresponding to the two different prime numbers a and b, and a prime number p corresponding to the Jacobian addition candidate value j, respectively based on the prime number a, the prime number b, and the size n of an encryption key [page 2, last paragraph and page 3 paragraphs 1 and 2];

an order candidate value computing procedure for computing a class H consisting of a plurality of candidate values for order of a Jacobian group of an algebraic curve specified by the prime number a and the prime number b, respectively based on the prime number a, the prime number b, and the Jacobian addition candidate value j [page 3 paragraphs 4 and 5, page 4 and page 5, paragraph 1];

a security judging procedure for searching for a candidate value h meeting a security condition such as almost prime number characteristic from the class H, according to the class H [page 7-8, section 3-5]; and

a parameter deciding procedure for computing a parameter of an algebraic curve whose order of the Jacobian group is in accord with the candidate value h, of the algebraic curves specified by the prime number a, the prime number b, and the prime number p, respectively based on the prime number a, the prime number b, the prime number p, and the candidate value h [page 8, section 3-5].

Duursma does not explicitly teach a stickelberger element computing procedure for computing a stickelberger element. However, Stevens teaches a method of computing stickelberger element in elliptic curves [page 75, paragraph 1 and page 88-92, section 3]. Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to include a method of computing a stickelberger element as per teachings of Stevens and implement it into the secure parameter generating method thought by Duursma, because such modification admits canonical parameterization allowing for a selection of secure parameters in algebraic curve cryptography.

10. As per claims 2 and19 the combination of Duursma and Stevens teaches the secure parameter generating method in an algebraic curve as applied above. But a storing means for storing different variables is not explicitly mentioned. However, Official notice is taken that it is well known to incorporate a storing means for storing different variables in order to perform calculations on the stored variables.

11. As per claims 3-17 and 20-34, the combination of Duursma and Stevens teaches the secure parameter generating method in an algebraic curve as applied above.

Furthermore, Duursma teaches said Jacobian addition candidate value computing procedure for generating a at random, which is an algebraic integer r generating a prime ideal of a cyclotomic K generated by the primitive ab root of 1 and whose absolute norm becomes the prime number p of bit length 2n/(a-1)(b-1) or so, based on the prime number a, the prime number b, and the size n of the encryption key and computing the Jacobian addition candidate value j by use of an equation [page 2, last paragraph and page 3 paragraphs 1 and 2]; said order candidate value computing procedure for computing a candidate value h for the order of the jacobian group of an algebraic curve specified by the parameters a and b [page 3 paragraphs 4 and 5, page 4 and page 5, paragraph 1]; said parameter deciding procedure for requiring the primitive a root, the primitive b root of 1 with prime number p used as a devisor [page 8, section 3-5]; and Stevens teaches Stickelberger element computing procedure for computing the Stickelberger element c by use of the equation w = Et [<t/a> + <t/b>] a_{t-1} based on the prime number a, and the prime number b [page 88-92, section 3].

12. As per claim 37, Duursma teaches a secure parameter generating method in algebraic curve cryptography comprising:

Jacobian addition candidate value computing procedure for generating a at random, which is an algebraic integer r generating a prime ideal of a cyclotomic K generated by the primitive ab root of 1 and whose absolute norm becomes the prime number p of bit length 2n/(a-1)(b-1), based on the prime number a, the prime number b, and the size n of the encryption key and computing the Jacobian addition candidate value j by use of an equation [page 2, last paragraph and page 3 paragraphs 1 and 2].

Duursma does not explicitly teach the jacobian addition candidate value based on a stickelberger element. However, Stevens teaches the jacobian addition candidate value based on a stickelberger element [page 75, paragraph 1 and page 88-92, section 3]. Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to include a method of computing the jacobian addition candidate value based on a stickelberger element as per teachings of Stevens and implement it into the secure parameter generating method thought by Duursma, because such modification admits canonical parameterization allowing for a selection of secure parameters in algebraic curve cryptography.

13. Claim 36 is rejected under 35 U.S.C. 103(a) as being unpatentable over Stevens (ref V).

14. As per claim 36, Stevens teaches a secure parameter generating method in algebraic curve cryptography comprising:

a stickelberger element computing procedure for computing the stickelberger element by use of the equation w = Et [<t/a> + <t/b>] a_{t-1} based on the prime number a and the prime number b [page 88-92, section 3]. However Stevens does not explicitly teach the variable t that runs on a typical series of irreducible residue class with ab used as a divisor. It would have been obvious to one having ordinary skill in the art at the time the invention was made to include a variable t that runs on a typical series of irreducible residue class with ab used as a divisor, in order to have a reduction method that generates secure parameters.

15. Claims 38 and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Duursma et al. (hereinafter Duursma) (ref U).

16. As per claim 38, Duursma teaches a secure parameter generating method in algebraic curve cryptography comprising:

order candidate value computing procedure for computing a candidate value h for the order of the jacobian group of an algebraic curve specified by the parameters a and b [page 3 paragraphs 4 and 5, page 4 and page 5, paragraph 1 and page7-8, section 3-5]. However, Duursma does not explicitly teach a Norm mapping. It would have been obvious to one having ordinary skill in the art at the time the invention was made to include a norm mapping into the secure parameter generating method thought by Duursma in order to compute a secure candidate value.

17. As per claim 39, Duursma teaches a secure parameter generating method in algebraic curve cryptography comprising:

parameter deciding procedure for requiring the primitive a root, the primitive b root of 1 with prime number p used as a devisor, based on the prime number a and the prime number b, and the prime number p and the candidate value h, generating a point G over an algebraic curve, computing the h-fold of an element in the Jacobian group indicated by the point G, and supplying p, as the parameter of an algebraic curve whose order of the jacobian group is in accord with the candidate value of h [pages 7-8, section 3-5, and pages 3-4, section 2-3]. However, Duursma does not explicitly teach the parameter of an algebraic curve whose order of the jacobian group is in accord with the candidate value of h if the result is equal to an identity element in the Jacobian group. It would have been obvious to one having ordinary skill in the art at the time the invention was made to include to include a parameter of an algebraic curve whose order of the jacobian group is in accord with the candidate value of h if the result is equal to an identity element in the Jacobian group in order to generate a secure parameter in algebraic curve.

Conclusion

18. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a) U.S. Patent No. 6,560,336 B1 to Arita

b) An addition algorithm in Jacobian of C34 curve, Seigo Arita

c) Addition in the Jacobian of a Curve over a finite field

d) On the performance of Hyperelliptic Cryptosystems.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Beemnet W Dada whose telephone number is (703) 305-8895. The examiner can normally be reached on Monday - Friday (8:30 am - 6:00 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y Vu can be reached on (703) 305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Beemnet Dada

April 26, 2004

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100